UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

ANGEL RODRIGUEZ, Individually, and on behalf of all others similarly situated, **Plaintiff** **v.** **VILLAGE PRACTICE MANAGEMENT COMPANY, LLC D/B/A VILLAGE MEDICAL D/B/A VILLAGEMD** **Defendant.**	**Civil Action No. 1:24-cv-02882**

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff, ANGEL RODRIGUEZ, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Second Amended Class Action Complaint against Defendant, VILLAGE PRACTICE MANAGEMENT COMPANY, LLC d/b/a VILLAGE MEDICAL d/b/a VILLAGEMD ("Village" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] ("PII")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

and/or Protected Health Information[2] ("PHI") (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), Microsoft Corp. ("Microsoft"), AdRoll, AppNexus, HubSpot, Frequence, the Trade Desk, and potentially others ("the Disclosure").

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendant's, that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[3] OCR and FTC agree that such tracking technologies, like those present on Defendant's website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[4] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Village is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services (July 20, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last accessed April 9, 2024), **attached as Exhibit A.**

[4] *Id.*

including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[5]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace and denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. In December 2022, HHS released a bulletin on its website regarding the use of tracking technologies by entities covered by HIPAA—healthcare entities like Village—and its

[5] *Id.*

business associates (the "December 2022 Bulletin").[6]

6. Therein, HHS defined tracking technologies, explaining:

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.[7]

7. In the Bulletin, HHS was clear in unambiguous terms that, "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[8,9]

8. On March 18, 2024, HHS updated its December 2022 bulletin, "to increase clarity for regulated entities and the public" and reiterating the above basic privacy obligations.[10,11]

---

[6] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 30, 2024).

[7] *Id*.

[8] *Id*. (bold emphasis in original)

[9] Citing *to* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").

[10] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. June 20, 2024).

[11] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern

9. Headquartered in Chicago, Illinois, Defendant is a massive medical system which provides treatment to patients in Illinois and across the United States, including in Colorado, Texas, Indiana, Kentucky, Michigan, Arizona, Georgia, Nevada, Florida, New Jersey, Rhode Island, Massachusetts, and New Hampshire.[12]

10. Despite its unique position as a massive and trusted healthcare provider, Defendant knowingly configured and implemented into its website, https://www.villagemedical.com/ (the "Website") code-based tracking devices known as "trackers" or "tracking technologies," which collected and transmitted patients' Private Information to Facebook, and other third parties, without patients' knowledge or authorization.

11. Defendant encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to learn about Village on its main website page,[13] to schedule appointments,[14] to find locations,[15] to find physicians and other medical providers,[16] to research treatment services,[17] to access a patient portal,[18] and more, including to research insurance information,[19] and to learn about health information via a blog.[20]

12. When Plaintiff and Class Members used Defendant's Websites and Online Platforms, they thought they were communicating exclusively with their trusted healthcare

---

District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

[12] https://www.villagemedical.com/locator (last accessed July 29, 2024).

[13] https://www.villagemedical.com/ (last accessed July 29, 2024).

[14] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. July 29, 2024).

[15] https://www.villagemedical.com/locator (last acc. July 29, 2024).

[16] https://www.villagemedical.com/our-providers (last acc. July 29, 2024).

[17] https://www.villagemedical.com/our-services (last acc. July 29, 2024).

[18] https://www.villagemedical.com/patient-portal (last acc. July 29, 2024).

[19] https://www.villagemedical.com/insurance (last acc. July 29, 2024).

[20] https://www.villagemedical.com/journey-to-well (last acc. July 29, 2024).

provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, Microsoft, AdRoll, AppNexus, HubSpot, Frequence, the Trade Desk, and possibly others into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

13. A tracker (also referred to as "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[21] When a person visits a website with an tracker, it tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[22] Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[23]

14. Among the trackers Defendant embedded into its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a website user's device and the URLs and domains they visit.[24] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[25] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to

[21] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

[22] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).

[23] *Id.*

[24] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).

[25] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).

be linked with their Facebook profile.[26]

15. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiff's and Class Members' private health information, alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

16. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[27]

17. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[28, 29]

---

[26] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

[27] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[28] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[29] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

18. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[30]

19. Defendant utilized data from these trackers to market their services and bolster their profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

20. On information and belief, the information that Defendant's Meta Pixel, and possibly CAPI, sent to Facebook included the Private Information that Plaintiff and the Class Members submitted to Defendant's Websites and Online Platforms, including, *inter alia*: their browsing activities including the pages they viewed and the buttons they clicked; their medical appointment booking activities; their searches for locations; their searches for physicians; and their statuses as patients, including that they were viewing medical services, and activities on the patient portal; as well identifying information, such as IP addresses and identifying cookies.

21. Such information allows third parties (e.g., Facebook) to learn of a particular individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then target Plaintiff and Class

[30] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

Members with online advertisements, based on the information they communicated to Defendant via the Website. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

22. In addition to the Facebook Pixel, and likely CAPI, on information and belief, Defendant installed other tracking technologies, such as Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk, which operate similarly to the Meta Pixel and transmitted Plaintiff's and Class Members' Private Information to unauthorized third parties.

23. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue.

24. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or other third parties uninvolved in their treatment.

25. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into its Website and servers, Defendant have never disclosed to Plaintiff or Class Members that it shared their Information with Facebook, Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, the Trade Desk, and possibly others.

26. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant. Defendant owed common law, statutory,

regulatory, and contractual duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

27. Upon information and belief, Village utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

28. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard their information from unauthorized disclosure.

29. Defendant breached its common law, statutory, and contractual obligations to Plaintiff and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patient web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

30. Plaintiff seeks to remedy these harms and brings causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Invasion of Privacy—Intrusion Upon Seclusion; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Implied Duty of Confidentiality; (VII) Violation of Illinois Consumer Fraud and Deceptive Business Practices Act,

("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.; (VIII) Violation of the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.; (IX) Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.;* (X) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service"); (XI) Violation of Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.; and (XII) Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

PARTIES

31. Plaintiff, ANGEL RODRIGUEZ, is a natural person and a resident and citizen of Massachusetts, where he intends to remain, with a principal residence in Quincy, Massachusetts in Norfolk County. Plaintiff has been a patient of Village since January 2023, and is a victim of Defendant's unauthorized Disclosure of Private Information.

32. Defendant VILLAGE PRACTICE MANAGEMENT COMPANY, LLC d/b/a VILLAGE MEDICAL d/b/a VILLAGEMD ("Village" or "Defendant"), is a limited liability company organized and existing under the laws of the State of Delaware, with a principal place of business located at 433 W. Van Buren Street, Suite 510 S. Chicago, Illinois 60607 in Cook County.[31]

33. Defendant's Registered Agent for Service of Process is Illinois Corporation Service Company, 801 Adlai Stevenson Drive, Springfield, Illinois 62703-4261.

JURISDICTION AND VENUE

34. This Court has personal jurisdiction over Defendant because, personally or through

[31] *See* Secretary of the Commonwealth of Massachusetts, Business Entity Summary, "Village Practice Management, LLC" available at https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=NrygV5fu.tPxNet6g3I21S_x5V.4vBXR40_T3cD5p.E- (last acc. Mar. 28, 2024).

its agents, Defendant operates, conducts, engages in, or carries on a business in this State; it maintains its principal place of business and headquarters in Illinois; and committed tortious acts in this State.

35. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendant.

36. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

37. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

COMMON FACTUAL ALLEGATIONS

A. Background

38. Defendant is an Illinois healthcare provider which renders primary care medical treatment to patients across the country under a mission "[t]o make primary care more caring."[32]

39. Village represents to patients and prospective patients that:

> **How we make you primary.**
>
> We take a "coordinated care" approach to your health. That means you receive the time and attention you need from an entire care team who coordinates with your primary care provider. This way, we can help you with annual check-ups, lab work, illness + injury treatment, even specialist referrals and medication management. And we welcome most insurance and Medicare Advantage plans.[33]

40. Defendant provides treatment services to patients in Illinois, as well as in Colorado, Texas, Indiana, Kentucky, Michigan, Arizona, Georgia, Nevada, Florida, New Jersey, Rhode

[32] https://www.villagemedical.com/ (last acc. July 29, 2024).
[33] *Id*.

Island, Massachusetts, and New Hampshire.[34]

41. In fact, as Village describes, "[o]ur teams live and work near our patients, in over 680 practices across cities, suburbs, and rural areas, including inside many Walgreens locations. This way we're never too far from your home. Or ours."[35]

42. Defendant's primary care medical services include: "Anywhere visits and same-day appointments" ("Get the care you need, when you need it. You can see a primary care provider at one of our practices, through a virtual visit on your phone or computer, or in-person at home for patients who need it."); Chronic care management ("We can help you manage a wide range of diseases including diabetes, hypertension, COPD (chronic obstructive pulmonary disease), congestive heart failure and endocrine disorders…"); " Coordination for your specialty care[;]" treatment for "Illness and injuries" ("We can help you take care of coughs, colds, the flu, ear infections and more. Before you head to urgent care, reach out for a phone consultation or same-day appointment."); as well as home care, Village Medical at Home; on-site laboratories; Annual Well Visits; and patient portal services, "24/7 account access" ("Schedule appointments, get reminders, view test and imaging results and more on your smartphone via the Village Medical Mobile App or on the web via your patient portal.").[36]

43. In fact, Village specifically promotes "Same-day appointments[;] Clinic, in-home & virtual visits[;]" and its convenient blood and other laboratory diagnostic testing:[37]

[34] https://www.villagemedical.com/locator (last acc. July 29, 2024).
[35] https://www.villagemedical.com/ (last acc. July 29, 2024).
[36] https://www.villagemedical.com/our-services (last acc. July 29, 2024).
[37] https://www.villagemedical.com/ (last acc. July 29, 2024).

44. According to Defendant, "Village Practice Management Company, LLC ('VillageMD' or 'We') is comprised of various entities that provide healthcare and related services to individuals throughout the United States of America. The following entities make up the VillageMD family: • Village Medical Primary Care Clinics* • Village Medical at Walgreens • Village Medical at Home • Village Medical Pharmacy [and] Village Medical Physical Therapy."[38]

45. On information and belief, Village "delivers services to around 1.6 million patients, […and] [i]ts 2021 revenue was about $1.3 billion…"[39]

46. Defendant serves many of its patients via its Websites and Online Platforms, which Village encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to learn about Village on its main website page,[40] to schedule appointments,[41] to find locations,[42] to find physicians and other medical providers,[43]

[38] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions **attached as Exhibit B.**

[39] Robert Holly, Home Health Care News, *VillageMD to Drive 'Tremendous Long-Term Growth' for Walgreens Health,* Jan. 14, 2022, avail. at https://homehealthcarenews.com/2022/01/villagemd-to-drive-tremendous-long-term-growth-for-walgreens-health/#:~:text=VillageMD%20delivers%20services%20to%20around,according%20to%20the%20investor%20deck. (last acc. July 29, 2024).

[40] https://www.villagemedical.com/ (last accessed July 29, 2024).

[41] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. July 29, 2024).

[42] https://www.villagemedical.com/locator (last acc. July 29, 2024).

[43] https://www.villagemedical.com/our-providers (last acc. July 29, 2024).

to research treatment services,[44] to access a patient portal,[45] and more, including to research insurance information,[46] and to learn about health information via a blog.[47]

47. Defendant promotes the comprehensive functionality of these tools and promotes their use, in service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely installed the Meta Pixel and other trackers such as Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, and the Trade Desk onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts and profits. But Defendant did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiff and Class Members, with Facebook, and those other unauthorized third parties.

48. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

49. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[48]

50. In conjunction with its advertising business, Facebook encourages and promotes its "Business Tools" to be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services.

51. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits

[44] https://www.villagemedical.com/our-services (last acc. July 29, 2024).
[45] https://www.villagemedical.com/patient-portal (last acc. July 29, 2024).
[46] https://www.villagemedical.com/insurance (last acc. July 29, 2024).
[47] https://www.villagemedical.com/journey-to-well (last acc. July 29, 2024).
[48] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

52. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[49] Businesses that want to target customers and advertise their services can also create their own tracking parameters by building a "custom event."[50]

53. The Meta Pixel is a Business Tool used to "track[] the people and type of actions they take" on a website.[51] When an individual accesses a webpage containing the Meta Pixel, the communications with that webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

54. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy, such as Defendant's "Provider" pages.[52]

55. The Meta Pixel's primary purpose is to enhance online marketing, improve online

---

[49] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[50] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[51] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

[52] https://www.villagemedical.com/our-providers (last acc. July 29, 2024).

ad targeting, and generate sales.[53].

56. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[54]

57. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[55]

58. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads

[53] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

[54] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

[55] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

by measuring what happens when people see them.[56]

59. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

60. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

61. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

62. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[57]

63. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

---

[56] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

[57] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

64. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

65. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

66. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

67. In this way, the Meta Pixel acts much like a traditional wiretap: intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

68. Separate from the Meta Pixel, third parties place cookies in the browsers of web users. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to identify users of a Meta-Pixel-enabled website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

69. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on

gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[58] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

70. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[59] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website server(s), in accordance with Facebook's documentation.

71. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

72. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, and others.

---

[58] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

[59] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

73. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

74. Consequently, when Plaintiff and Class Members visited Defendant's Websites and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

iii. Defendant's Other Trackers: Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk

75. On information and belief, Defendant also employed other trackers which likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization, including Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk.

76. Most basically, "Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business."[60] Once a business implants the Google Analytics tracking measurement code on a its website, every time a user visits a webpage, the tracking code will collect information about how that user interacted with the page.[61]

77. Google Analytics allows Defendant to track and share with Google (1) who uses its website; (2) what is performed on its website; (3) when users visit its website; (4) where on

[60] Google, *Analytics Help, Introduction to Analytics How Google Analytics works*, avail. at https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=3016588406699844463-NC

[61] *Id*.

the website users perform these actions; and (5) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on WH's Website and generates corresponding reports.[62]

78. To help Google generate reports (usually in realtime), trackers embedded in a website send Google (1) information about the user's device; (2) client- and user-specific identifiers; and (3) information about what event the user performed.

79. According to Google, "Google Tag Manager is a tag management system (TMS) that allows you to quickly and easily update measurement codes and related code fragments collectively known as ***tags*** on your website or mobile app. Once the small segment of Tag Manager code has been added to your project, you can safely and easily deploy analytics and measurement tag configurations from a web-based user interface."[63]

80. As Google goes onto describe:

> When Tag Manager is installed, your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web-based user interface to set up tags, establish ***triggers*** that cause your tag to fire when certain events occur, and create ***variables*** that can be used to simplify and automate your tag configurations.
>
> A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a ***container***. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.[64]

[62] *See generally*, MarketLytics, *A big list of what Google Analytics can & cannot do*, avail. at https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/

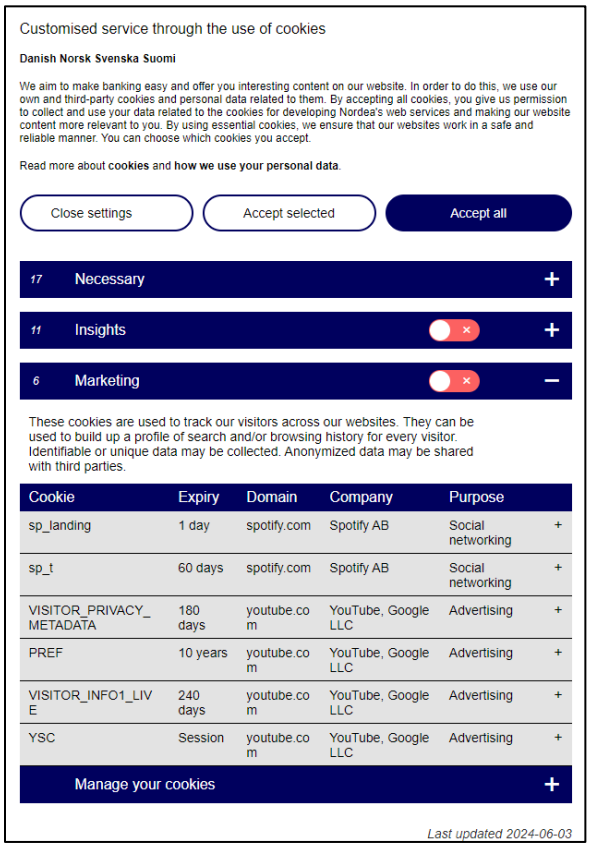
[63] *See Google Tag Manager Overview,* available at https://support.google.com/tagmanager/answer/6102821?hl=EN#:~:text=Google%20Tag%20Manager%20is%20a,your%20website%20or%20mobile%20app (last acc. June 26, 2024).

[64] *Id*.

81. Defendant also utilizes Double Click Ads. Google's DoubleClick is "an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."[65]

82. DoubleClick includes DoubleClick Digital Marketing Manager ("Ad serving and management solutions for your digital advertising campaigns, including trafficking and reporting"), Google Analytics, and more.[66]

83. Information gathered through DoubleClick can be used by Google to personalize the advertisements users are targeted with across the web. *See*, e.g., https://www.nordea.com/en/doubleclick-cookies:



Customised service through the use of cookies

Danish Norsk Svenska Suomi

We aim to make banking easy and offer you interesting content on our website. In order to do this, we use our own and third-party cookies and personal data related to them. By accepting all cookies, you give us permission to collect and use your data related to the cookies for developing Nordea's web services and making our website content more relevant to you. By using essential cookies, we ensure that our websites work in a safe and reliable manner. You can choose which cookies you accept.

Read more about **cookies** and **how we use your personal data**.

Close settings | Accept selected | Accept all

17 Necessary +

11 Insights +

6 Marketing −

These cookies are used to track our visitors across our websites. They can be used to build up a profile of search and/or browsing history for every visitor. Identifiable or unique data may be collected. Anonymized data may be shared with third parties.

Cookie	Expiry	Domain	Company	Purpose	
sp_landing	1 day	spotify.com	Spotify AB	Social networking	+
sp_t	60 days	spotify.com	Spotify AB	Social networking	+
VISITOR_PRIVACY_METADATA	180 days	youtube.com	YouTube, Google LLC	Advertising	+
PREF	10 years	youtube.com	YouTube, Google LLC	Advertising	+
VISITOR_INFO1_LIVE	240 days	youtube.com	YouTube, Google LLC	Advertising	+
YSC	Session	youtube.com	YouTube, Google LLC	Advertising	+

Manage your cookies +

Last updated 2024-06-03

[65] Google Help, DoubleClick Digital Marketing, avail. at https://support.google.com/faqs/answer/2727482?hl=en (last acc. June 26, 2024).

[66] *Id*.

84. Defendant also utilizes Microsoft Universal Events, which allows business such as Defendant to "[t]rack what your customers are doing after they click on your ad."[67]

85. As Microsoft goes onto explain, "Universal Event Tracking (UET) is a powerful tool that records what customers do on your website. By creating one UET tag and placing it across your website, Microsoft Advertising will collect data that allows you to track conversion goals and target audiences with remarketing lists."

86. Microsoft touts the benefits of UET as enabling businesses to:

> **Maximize returns**
>
> This approach allows you to optimize the overall value obtained from the conversions you achieve. By incorporating Target Return on Ad Spend (tROAS), you have an extra level of control to ensure that you generate the maximum possible conversion value or revenue while maintaining an adequate return on your ad spend.
>
> **Maximize conversions**
>
> Focused on achieving the maximum number of conversions within the limits of your budget. By incorporating Target CPA (tCPA), you gain an extra level of control that allows you to optimize the number of conversions while keeping the cost per acquisition at a desired level.
>
> **Precise audience targeting**
>
> A technique that allows advertisers to reach a specific audience by using a combination of data and technology to deliver personalized messages to the right people. This can be achieved through various methods such as retargeting, contact targeting, and predictive targeting.[68]

87. Village too utilized HubSpot, "an AI-powered customer platform with all the software, integrations, and resources you need to connect your marketing, sales, and customer

[67] *Microsoft Advertising*, available at https://about.ads.microsoft.com/en/tools/performance/conversion-tracking#:~:text=Universal%20Event%20Tracking%20(UET)%20is,target%20audiences%20with%20remarketing%20lists (last acc. June 26, 2024).

[68] *Id*.

service. HubSpot's connected platform enables you to grow your business faster by focusing on what matters most: your customers."[69]

88. As described by AgencyAnalytics, "HubSpot Analytics provides a detailed view of customer interactions across various channels. It effectively tracks and analyzes every touchpoint in the customer journey, turning raw data into valuable insights. This process is crucial for identifying trends, optimizing strategies, and improving overall marketing performance."[70]

89. Defendant too uses AdRoll, whose marketing analytics features can assist businesses to do the following, along with much more:

> **Build your audience**
>
> Using our pixel and machine learning data engine, we create optimal audience segments based on behavior and interest. Already know who your best customers are? Input custom audience parameters and we'll continually add users who fit the bill.
>
> **Follow the customer journey**
>
> In a glance or with one simple download, get a visual report of customer touchpoints on their path to conversion.[71]

90. Moreover, Defendant uses AppNexus, now Xandr, which on information and belief is owned by Microsoft.

91. Further, Defendant utilized Frequence. Frequence is a digital advertising platform that combines all aspects of building a media strategy, including targeted advertising and reporting on the success of ad campaigns.

---

[69] https://www.hubspot.com/ (last acc. July 29, 2024).

[70] AgencyAnalytics, *31 Essential Hubspot Metrics to Track for Clients*, avail. at https://agencyanalytics.com/blog/hubspot-metrics (last acc. July 22, 2024).

[71] AdRoll, *Analytics*, avail. at https://www.adroll.com/features/analytics (last acc. July 29, 2024).

92. Lastly, Defendant utilizes Trade Desk which, "…[o]ffers advanced targeting based on demographics, behaviors, interests, and more. It also provides cross-device tracking through its Unified ID solution, ensuring a consistent view of users across devices."[72]

93. Frequence likely uses the data collected by Facebook and the other trackers to target advertising to Defendant's website users as well as provide analysis on ad campaign performance.

94. On information and belief, through these other trackers, Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk, Defendant transmitted Plaintiff's and the Class Members' Private Information to Facebook and those other third parties without Plaintiff's and Class Members' knowledge or authorization.

iv. Defendant Violated Its Own Privacy Policies

95. Defendant maintains and is covered under a Joint Notice of Privacy Practices,[73] ("Notice of Privacy Practices") and a website Terms of Use[74] (collectively, "Privacy Policies") which are posted on its Website.

96. Defendant's Notice of Privacy Practices "applies to the following organizations (collectively, "Village Medical"): • Village Medical and its medical staff • Village Medical Physical Therapy and Rehabilitation and its medical staff • Village Medical at Home and its medical staff • Village Medical Pharmacy and its medical staff."[75]

---

[72] Improvado, https://improvado.io/blog/trading-desk-guide#:~:text=The%20Trade%20Desk%3A%20Offers%20advanced,search%20history%20and%20browsing%20behavior (last acc. July 22, 2024).

[73] Village, *Joint Notice of Privacy Practices*, avail. at https://www.villagemedical.com/hubfs/Documents/Compliance/VMD%20NPP%20-%201-30-2024.pdf (last acc. July 29, 2024), **attached as Exhibit C.**

[74] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions (last acc. July 29, 2024), **Exhibit B.**

[75] *Joint Notice of Privacy Practices*, **Exhibit C.**

97. In the Notice of Privacy Practices, Village represents, acknowledges, and promises patients that:

> Law requires us to keep your identifiable health information private, to provide you with this Notice of our legal duties and privacy practices with respect to your health information and to follow the terms of the Notice as long as it is in effect. If we revise this Notice, we will follow the terms of the revised Notice, as long as it is in effect.[76]

98. Therein, Defendant enumerates certain purposes for which it may disclose health information/Private Information, *inter alia*: for treatment ("We may use or disclose your health information to a physician or other healthcare provider in order to provide care and treatment to you…"); payment; for healthcare operations ("We may use or disclose health information about you to support the programs and activities of Village Medical, such as quality and service improvement, healthcare delivery review, staff performance evaluation, competence or qualification review of healthcare professionals, education and training of physicians and other healthcare providers, business planning and development, business management and general administrative activities…); in a health information exchange; to family and friends; for public health and safety purposes as described; to business associates ("There are some services provided at Village Medical through contracts with business associates. When these services are contracted, we will disclose your health information to the business associate so they can perform the job we have asked them to do. However, business associates, such as Village Medical, are required by federal law to appropriately safeguard your information."); and for research purposes.[77]

99. None of the purposes for which Village may disclose PHI/health information without written authorization under the Notice of Privacy Practices include the Disclosure of

[76] *Id.*
[77] *Id.*

Private Information via the Meta Pixel and other trackers to third parties for marketing purposes.

100. Further, in the Notice of Privacy Practices, Defendant specifically represents, acknowledges, and promises that, "[w]e will not use or disclose your health information, except as described in this document, unless you authorize us, in writing, to do so. […] Specific examples of uses or disclosures requiring written authorization include the use of psychotherapy notes, marketing activities, the sale of your health information and most uses and disclosures for which we are compensated."[78]

101. Moreover, therein, Village states that, "[i]n certain instances, you have the right to be notified in the event that we, or one of our business associates, discover an inappropriate use or disclosure of your health information. Notification of any such use or disclosure will be made in accordance with state and federal requirements."[79]

102. In addition, Defendant maintains a Website Terms of Use, in which Village states:

> Welcome! You have arrived at a website or application (collectively, a "Digital Service") location which is owned and operated by Village Practice Management Company, LLC ("VillageMD" or "We"). […]
>
> This Terms of Use governs your access to and use of the Digital Service, including any content, functionality and services offered on or through the Digital Service. **Please read these Terms of Use carefully before accessing or using the Digital Service, so that you fully understand your rights and responsibilities**.[80]

103. In fact, in the Terms of Use, Village specifically represents and promises that "[t]he use of the Digital Service is also governed by the terms of the VillageMD Privacy Policy which are incorporated into these Terms of Use by this reference. Any protected health information

---

[78] *Id*.
[79] *Id*.
[80] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions (last acc. July 29, 2024), **Exhibit B** (bold emphasis added)

collected on the Digital Service will be used and disclosed only in accordance with VillageMD's Notice of Privacy Practices. By using the Digital Service, you consent to all actions taken by us with respect to your information in compliance with the Privacy Policy." [81]

104. In the Terms of Use, Defendant states that it "has business relationships and affiliations with third-party vendors that deliver certain services and content" which include Google Analytics ("We use Google Analytics for tracking queries submitted to ***their*** search engines. We also use Google's DoubleClick technology for tracking our advertisements, enabling "tell-a-friend" social media functionality and providing us with the contact information of users who submit a request for additional information about our services via click-through advertisements…") and Cision, but does not mention Facebook.[82]

105. Nowhere in the Terms of Use does Village disclose its use of the Meta Pixel, or that it will share patients' Private Information, including PHI, with third parties uninvolved in their treatment, for marketing purposes, without their authorization.

106. Nowhere in the Terms of Use does Village disclose that other trackers such as Google Analytics, Google Tag Manager, Google DoubleClick Ads, or others such as Microsoft, AdRoll, AppNexus, HubSpot, Frequence, or the Trade Desk, will, in reality, disclose their Private Information, including PHI, to those third parties, including Facebook.

107. Despite these representations in its Privacy Policies, Defendant does indeed transfer Private Information to third parties for marketing purposes, without written authorization. On information and belief, using the Meta Pixel and other tracking technologies, such as Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot,

[81] *Id*.
[82] *Id*. (bold italicized emphasis added).

AdRoll, AppNexus, Frequence, and The Trade Desk, Defendant used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, Google, Microsoft, and those other unauthorized third parties, without written authorization, in violation of Village's Privacy Policies.

v. Village Unauthorizedly Disclosed Plaintiff's and the Class's Private Information

108. Defendant disclosed Plaintiff's and Class Members' Private Information and confidential communications to Facebook and other third parties via the Meta Pixel and other tracking technologies for marketing purposes.

109. On information and belief, through the use of the Meta Pixel, Defendant disclosed to Facebook the Private Information and communications that Plaintiff and the Class Members submitted to Defendant's Website including, *inter alia*: their browsing activities including the pages they viewed and the buttons they clicked; their medical appointment booking activities; their searches for locations; their searches for physicians; and their statuses as patients, including that they were viewing medical services, and their activities on the patient portal; as well identifying information, such as IP addresses and identifying cookies.

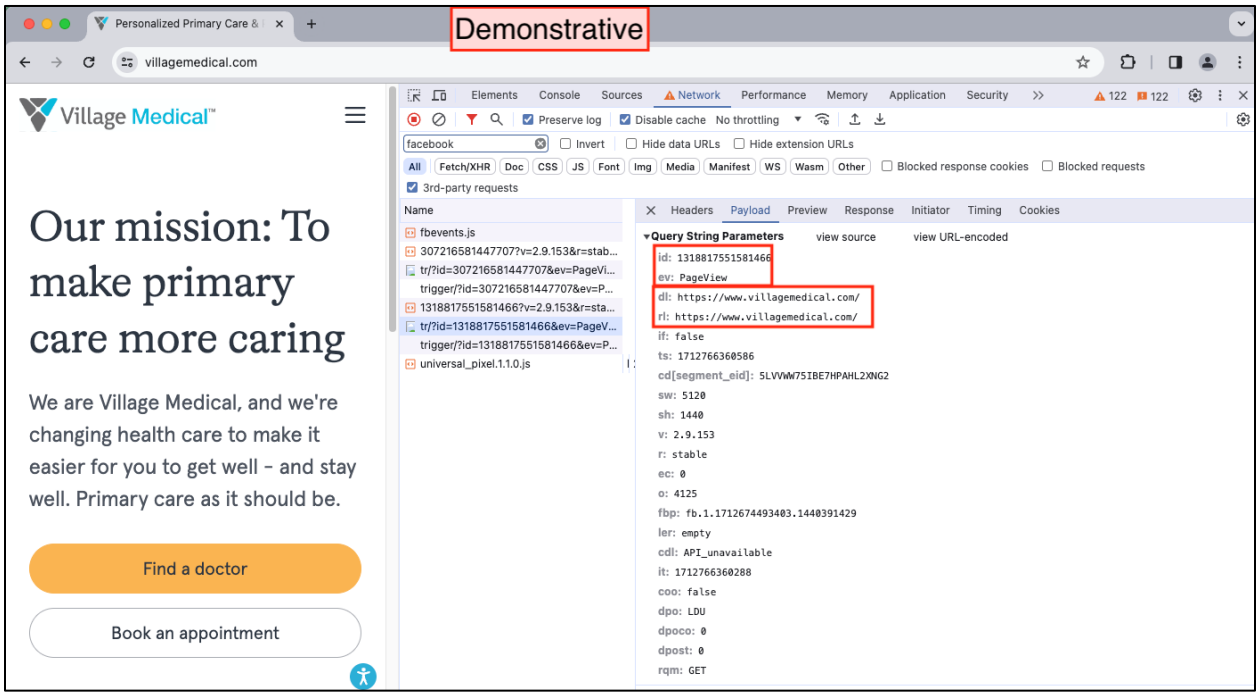
110. Since at least June 6, 2020, at the inception of the Website, Village has installs one Meta Pixel via a Google Tag Manager container, and has installed a second Meta Pixel to track PageView, Lead, Contact, and ViewContent events. Moreover, as of November 30, 2023, Village previously installed a third Meta Pixel via AdRoll.

111. Accordingly, Village disclosed its patients'—including Plaintiff's and the Class Members'—data and Private Information to Facebook from at least as early as June 6, 2020 through at least April 11, 2024.

112. By way of example, as configured as of November 30, 2023, Defendant's Meta Pixel and/or its Pixel loaded by AdRoll's roundtrip.js file, disclosed the following to Facebook:

Village used its Meta Pixels to Track Patients' Browsing Activities Across its Website.

113. Upon a patient's arrival on Village's homepage, Village would send a PageView event disclosing that the patient loaded the page at URL "https://www.villagemedical.com/.":



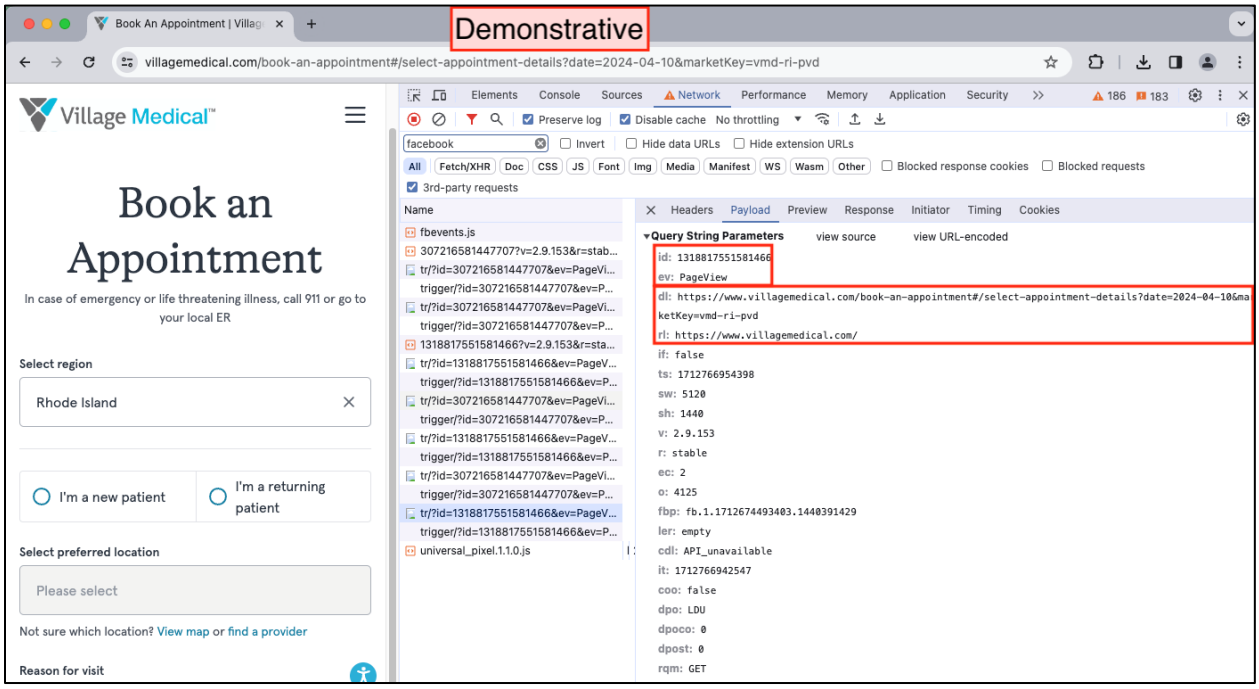
114. As patients browsed Village's website beyond the homepage, Village continued to disclose information about patients using the Online Platforms to Facebook.

115. Through Village's transmission of PageView, FindLocation, and EventSegment events, Village disclosed information about patients': (i) appointment booking activities; (ii) location and physician searches; and (iii) other activities that revealed users' statuses as patients.

Village Disclosed Patients' Appointment Booking Activities

116. As patients booked appointments on Village's website, Village would send Facebook PageView events disclosing the patients' activities.

117. For instance, when a patient selected Rhode Island to book an appointment, Village would send a PageView event with the URL "https://www.villagemedical.com/book-an-appointment#/select-appointment-details?date=2024-04-10&marketKey=vmd-ri-pvd.":



118. The "marketKey" indicates the patient is booking an appointment in the Rhode Island, Providence area.

119. Next the patient is prompted to indicate whether they are an existing patient or not. If the patient selected "I'm a returning patient," Village would transmit a PageView event with the URL "https://www.villagemedical.com/book-an-appointment#/select-appointment-details?date=2024-04-11&marketKey=vmd-ri-pvd&isExistingPatient=true," disclosing the Facebook that the user was an existing patient.

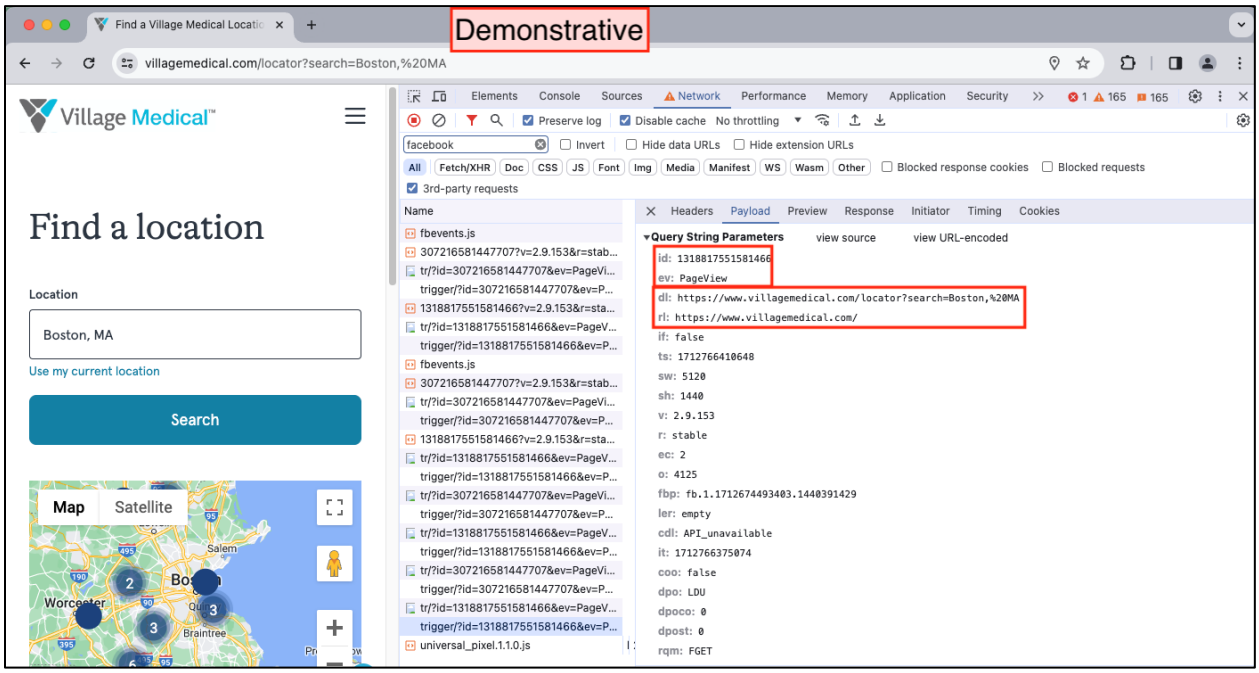
120. As the patient selects a date to schedule an appointment, Village would send a PageView event with the URL "https://www.villagemedical.com/book-an-appointment#/select-appointment?date=2024-04-14&marketKey=vmd-ri-pvd&isExistingPatient=true&departmentId=40&reasonId=51" where the date parameter now indicates the appointment date.

Village Disclosed Patients' Searches for Locations and for Physicians and Other Providers

121. Village also disclosed patients' searches for a location or physician.

122. For example, when a patient went to the Find a location page, Village would transmit a PageView event reporting to Facebook that the patient was on the page at "https://www.villagemedical.com/locator."

123. Village would send another PageView event disclosing when the patient searched for a specific location, as shown below:



124. For instance, if the patient searched for offices in Boston, MA, the PageView event would inform Facebook that the patient "search[ed]=Boston,%20MA."

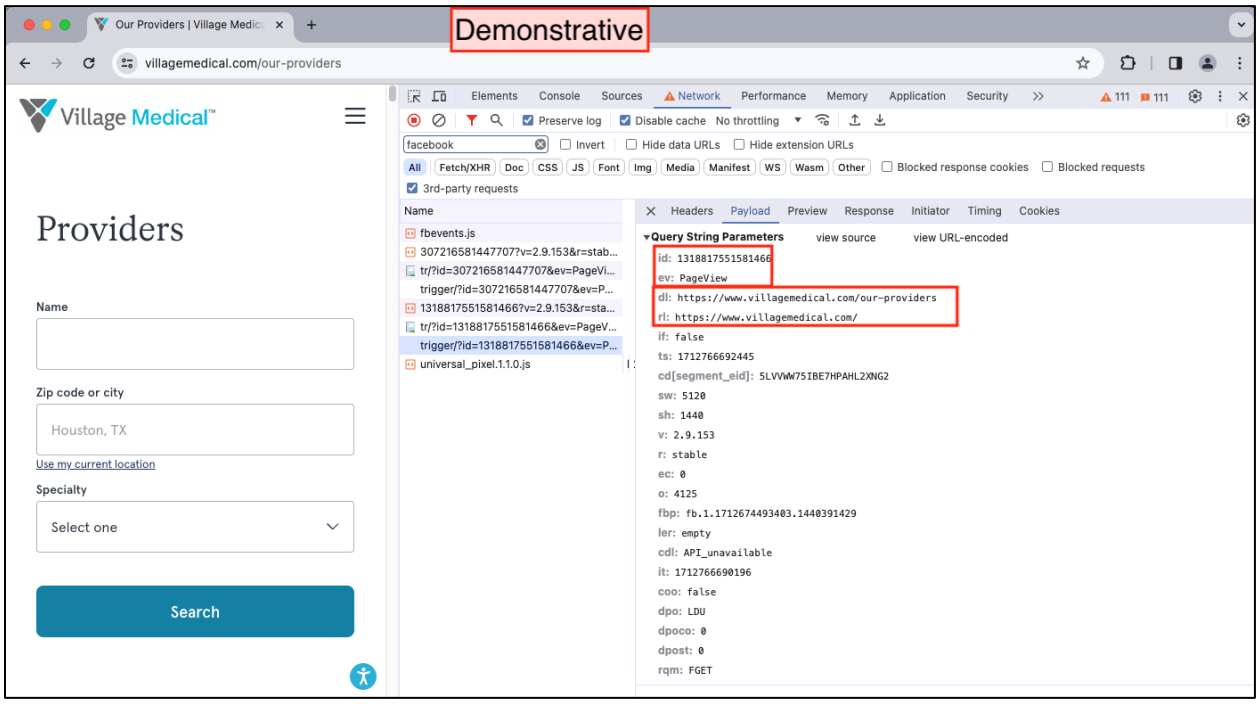
125. Then, as the patient selected a location, Village would send PageView and FindLocation events.

126. The PageView event would provide Facebook with the location of the facility selected.

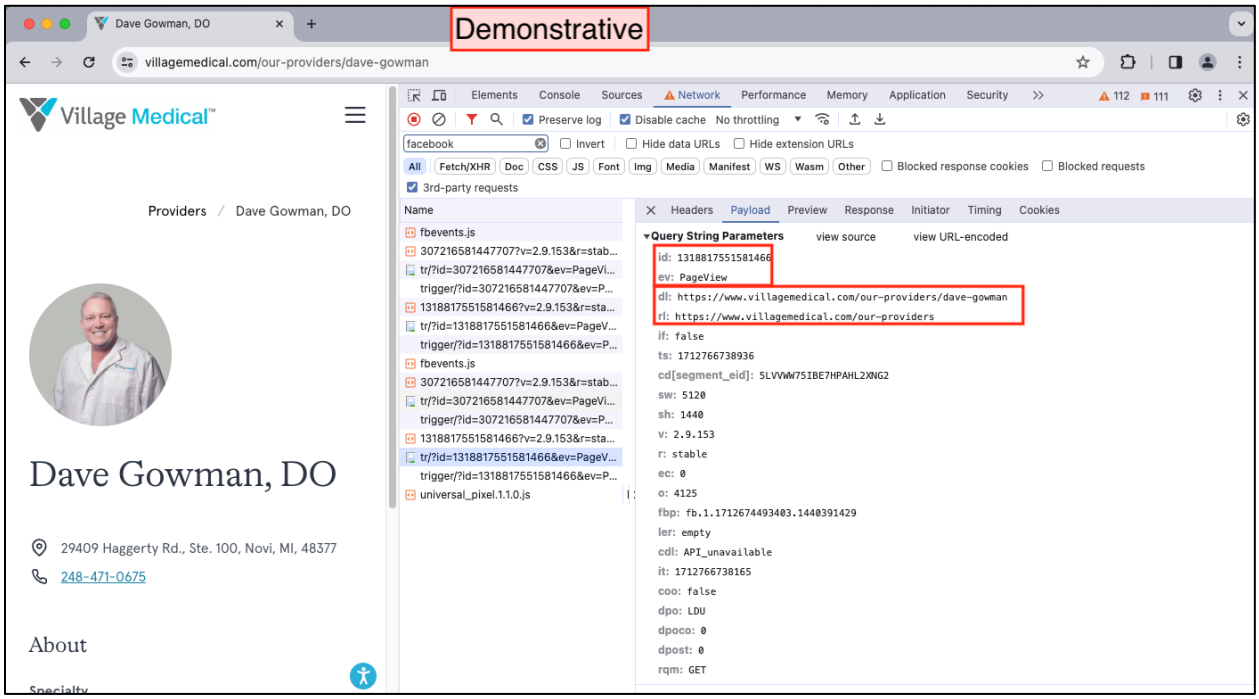
127. For instance, if the patient selected the Brookside Medical location, the PageView event would indicate the patient was viewing a location at "106-nate-whipple-highway-cumberland-ri-02864."

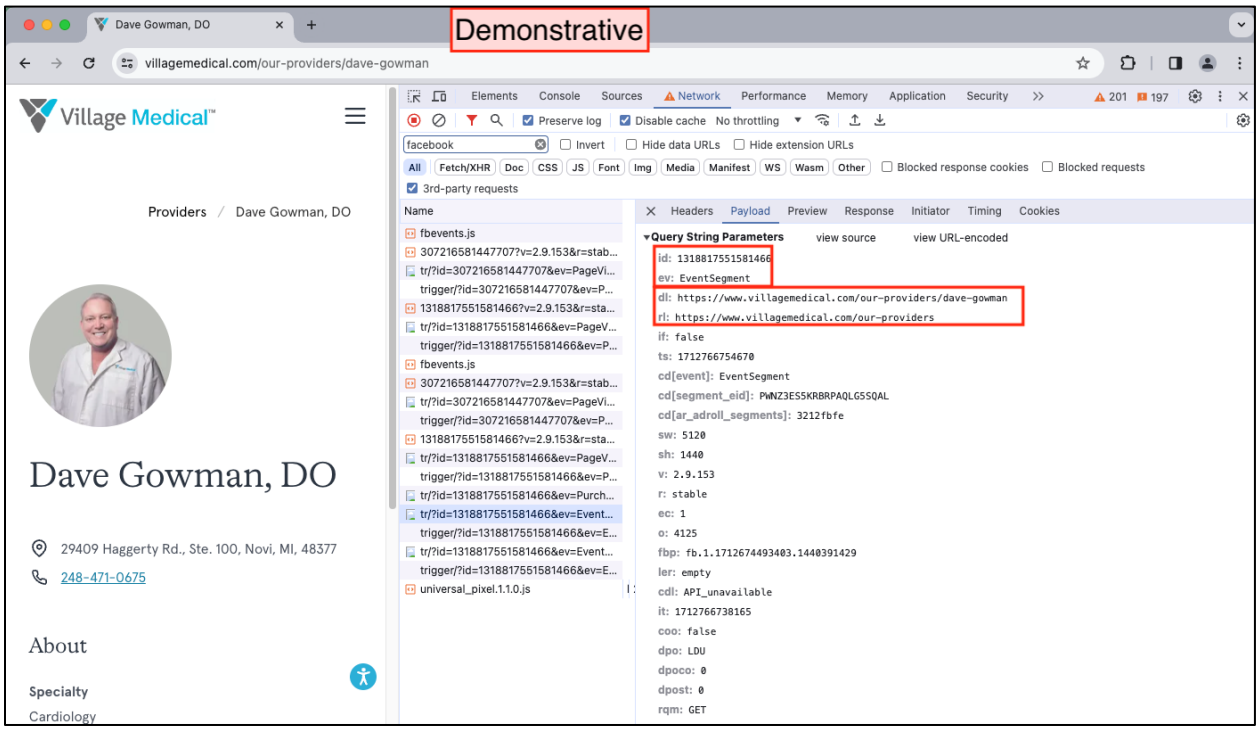
128. Village also disclosed details of patients' physician searches to Facebook.

129. The disclosures began with a PageView event revealing when a patient viewed the page at "https://www.villagemedical.com/our-providers.":



130. Then when the patient clicked to learn more about a provider, Village would send PageView and EventSegment events. Both events inform Facebook the name of the provider the patient is learning about. The disclosure is illustrated below:



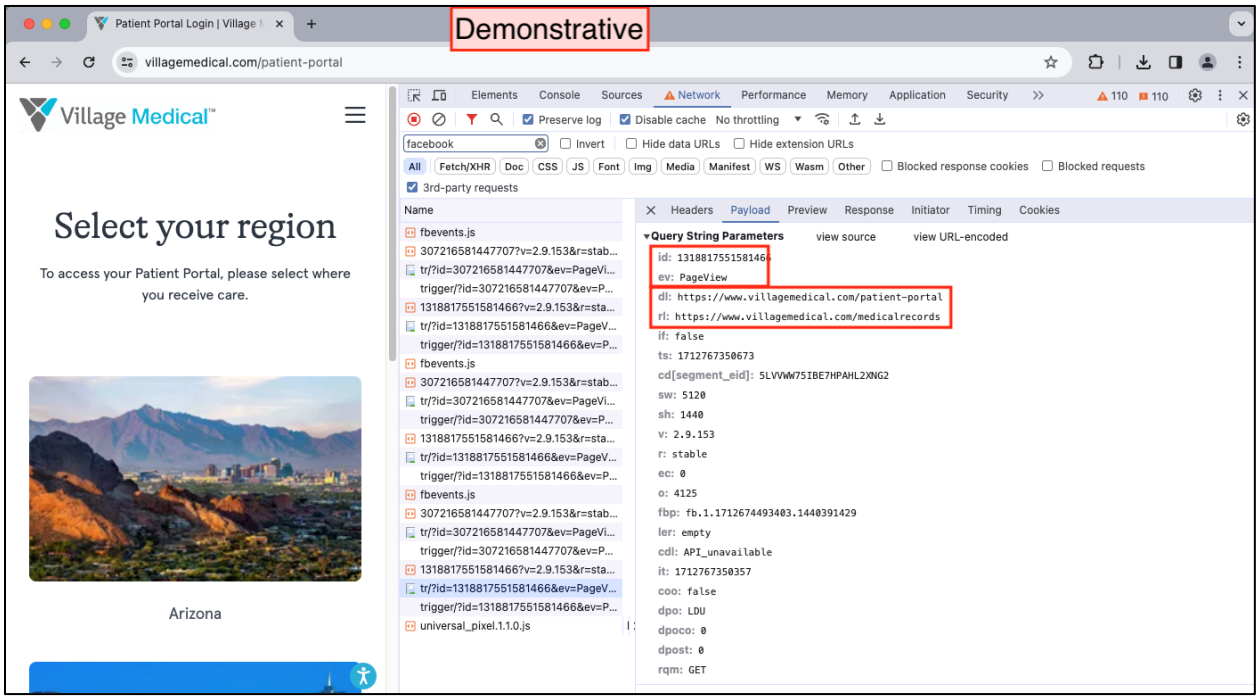


Village Disclosed Patients' Activities That Revealed Their Statuses as Patients, Including Use of the Patient Portal, the Medical Services Page, and for Medical Records

131. Village also disclosed patients' activities that would reveal their patient status, including use of the patient portal, the medical service pages, and for medical records.

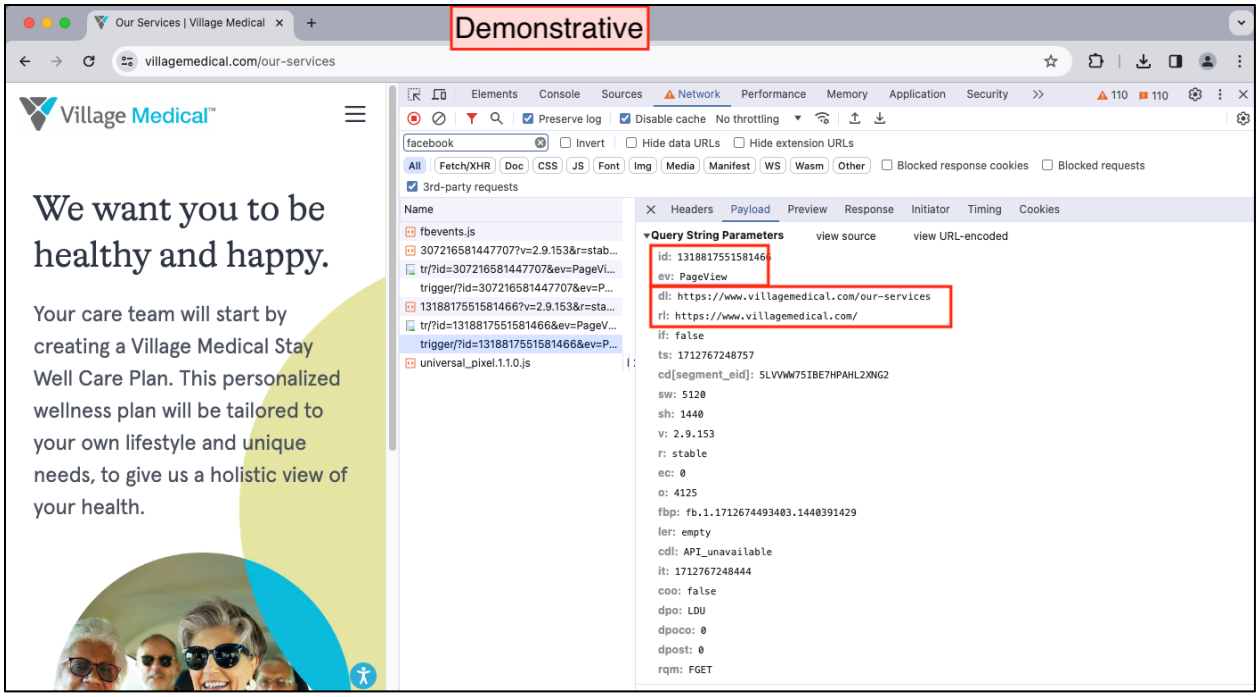
132. For instance, Village would disclose as a patient navigated to find the patient portal by sending a PageView event.

133. The event would reveal the patient was viewing the page at URL "https://www.villagemedical.com/patient-portal.":



134. Village also disclosed when patients visited the medical records page which triggered Village to send a PageView event informing Facebook the patient was viewing "https://www.villagemedical.com/medicalrecords."

135. Similarly, Village disclosed when a patient viewed the Services page with a PageView event that included the URL "https://www.villagemedical.com/our-services."



Defendant Disclosed Patients' Identifying Information

136. Lastly, in addition to this information, Defendant disclosed patients' identifying information, including their IP addresses and identifying cookies, and/or Facebook ID.

137. In each of the Facebook events that Village sent to Facebook, Defendant included the "c_user" cookie, which Facebook uses to identify users.

138. Facebook can therefore connect cookie data that Village transmitted with specific patients using the Online Platforms.

139. Furthermore, Facebook's "Your activity off Meta technologies" report confirms that Facebook would have received the data Village shared with Facebook.

140. On information and belief, through the Meta Pixel installed and used by Defendant, Village collected and transmitted interactions of patients—Plaintiff and the Class Members—with Defendant's Website, and sent records of those interactions to Facebook. For example, when a patient visited Defendant's Website and the Providers page and searched for physicians, e.g., a

primary care physician for Plaintiff, and then clicked on the provider, the individual's browser sends a request to Defendant's server requesting that it load the webpage. Then, Meta Pixel sends secret instructions back to the individual's browser, causing it to imperceptibly record the patient's communication with Defendant and transmit the particular physician's page viewed by the patient to Facebook's servers, alongside the patient's IP address, the "c_user" cookies and/or sometimes the patient's unique Facebook ID. Thus, the services patients viewed, alongside identifying information, is reported back to Facebook, thereby revealing the patient's Private Information.

141. Defendant could have chosen not to use the Meta Pixel, or other tracking technologies such as Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk, or it could have configured it to limit the information that it communicated to Facebook and the other third parties, but it did not. Instead, on information and belief, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiff's and Class Members' Private Information.

142. Defendant used and disclosed Plaintiff's and Class Members' Private Information to Facebook, Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, the Trade Desk, and possibly others, for the purpose of marketing its services and increasing its profits and reducing its marketing costs.

143. On information and belief, Defendant shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook in exchange for improved targeting and marketing services and reduced marketing costs.

144. Plaintiff and the proposed Class Members never consented, agreed, authorized, or otherwise permitted Defendant to intercept their communications or to use or disclose their Private

Information for marketing purposes. Plaintiff and the proposed Class Members, patients of Defendant, were never provided with any written notice that Defendant disclosed its patients' Protected Health Information to Facebook, or other third parties including Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, the Trade Desk, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's and Class Members' Private Information including Protected Health Information to unauthorized entities.

145. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

146. Furthermore, Defendant actively misrepresented it would preserve the security and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant shared data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiff and Class Members, such as their IP addresses and identifying cookies.

147. By law, Plaintiff and the Class Members are entitled to privacy in their Private Information, including Protected Health Information, and confidential communications. Village deprived Plaintiff and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook, and likely others; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

B. Plaintiff's Experience

148. Plaintiff has been a patient of Defendant since January 2023, approximately, receiving healthcare services from Village and physicians in Village's network, including for primary care including mental health treatment at Defendant's clinic in Quincy, Massachusetts.

149. Plaintiff used Village's Website and Online Platforms beginning in January 2023, and last in October 2023, approximately one time per month, to facilitate his personal medical care with Defendant.

150. Plaintiff used the Website and Online Platforms to: browse the Website; to find a doctor on the "Find a provider" function, *to wit*, the names of his primary care and family practice providers, including for his mental health;[83] to search for practice locations closer to his home;[84] to research treatments for mental health and primary care; and Plaintiff used the patient portal, including to schedule appointments.[85]

151. Plaintiff is a Facebook user since 2012 or 2013. After Plaintiff used Defendant's Online Platforms, on or about June 2023, advertisements for Village Medical, and for mental health outpatient clinics from Defendant began appearing in his Facebook feed. At approximately the same time, Plaintiff also began to see advertisements related to ADHD and depression treatment.

152. Plaintiff relied on Defendant's Website and Online Platforms to communicate confidential patient information. He discovered that Defendant was unauthorizedly disclosing his Private Information to Facebook via the Meta Pixel, and to others via other trackers, in December 2023.

[83] https://www.villagemedical.com/our-providers (last acc. July 29, 2024).
[84] https://www.villagemedical.com/locator (last acc. July 29, 2024).
[85] https://www.villagemedical.com/patient-portal (last acc. July 29, 2024).

153. Plaintiff accessed Defendant's Website and Online Platforms at Defendant's direction and encouragement.

154. Plaintiff reasonably expected that his communications with Village were confidential, solely between himself and Village, and that, as such, those communications would not be transmitted to or intercepted by a third party.

155. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to Village's Privacy Policies and the law.

156. Plaintiff never intended to sell his Private Information nor would he have permitted it to be made available for sale on the resale market.

157. On information and belief, through its use of the Meta Pixel on the Online Platforms, Defendant disclosed to Facebook:

a. Plaintiff's browsing activities, including the pages and content Plaintiff viewed;

b. Plaintiff's seeking of medical treatment;

c. Plaintiff's searches for treatment locations;

d. Plaintiff's location via the zip code he searched;

e. Plaintiff's searches for primary care and/or family medicine physicians and other medical providers, including the names of the physicians he searched for and viewed, and/or their specialties;

f. The mental health and primary care treatments Plaintiff viewed;

g. Plaintiff's status as a patient, including his views of Defendant's medical services page, and of the Patient Portal login page;

h. Other information concerning Plaintiff's use of the patient portal, including

to schedule appointments; and

i. Plaintiff's identity via his IP addresses, "c_user" cookies or Facebook ID.

158. By failing to receive the requisite consent, Village breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

159. As a result of Village's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of his Private Information; unauthorized access of his Private Information by third parties;

b. Plaintiff now receives targeted health-related advertisements on Facebook, reflecting his private medical treatment information;

c. Plaintiff paid Village for medical services and the services he paid for included reasonable privacy and data security protections for his Private Information, but Plaintiff did not receive the privacy and security protections for which he paid, due to Defendant's Disclosure;

d. The portion of Village's revenues and profits attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

e. The portion of Village's savings in marketing costs attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

f. The portion of Village's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting

Plaintiff's Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff of surrendering his choice to keep his Private Information private and allowing Village to track his data;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff's Private Information;

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of his Private Information; and

l. Statutory damages.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

160. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[86] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

161. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he

[86] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective…at preventing the receipt of sensitive data."[87]

162. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[88] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[89]

163. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[90]

---

[87] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.

[88] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

[89] *Id.*

[90] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022)

164. In June 2022, an investigation by The Markup[91] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[92] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[93] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[94]

165. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[95]

166. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[96]

---

https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

[91] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed June 21, 2024).

[92] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

167. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[97]

D. Defendant Violated HIPAA Standards

168. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[98]

169. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

170. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[99]

171. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or his protected health information

[97] *Id.*

[98] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[99] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

> can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[100]

172. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology (the "December 2022 Bulletin").[101]

173. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[102]

174. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft,

[100] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[101] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited June 21, 2024).

[102] *Id.*

> financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [103]

175. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendant Violated FTC Standards, and the FTC and HHS Take Action

176. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[104]

177. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[105]

178. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible

---

[103] *Id.* (emphasis in original) (internal citations omitted).

[104] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **Exhibit A.**

[105] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

disclosures of PHI to third parties or any other violations of the HIPAA Rules"[106] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[107]

179. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[108]

180. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[109]

---

[106] *Id.*

[107] *Id.*

[108] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

[109] *See, e.g., U.S. v. Easy Healthcare Corp.,* Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.,* FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc*; In the Matter of Flo Health*

181. As such, the FTC and HHS have expressly stated that conduct like Defendant's runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

182. On March 18, 2024, HHS updated its December 2022 bulletin in the "March 2024 Bulletin," expanding the circumstances in which HHS would consider information from any unauthenticated website visitor to be considered PHI, and its disclosure to be a violation of HIPAA.[110,111]

183. The March 2024 Bulletin added guidance on when the disclosure of individually identifiable health information ("IIHI") is impermissible under HIPAA, explaining that: "the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute IIHI ***if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care***."[112]

184. However, in contrast, when a user visits a website related to his or her past, present, or future health, health care, or payment for health care, such as "…looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other

---

Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

[110] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. June 21, 2024).

[111] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

[112] *Supra,* n.151 (bold, italicized emphasis added).

identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care[,]" such that the disclosure of their information would be PHI, HIPAA rules apply, and that disclosure would be a violation of HIPAA.[113]

F. Defendant Violated Industry Standards

185. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

186. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Village and its physicians.

187. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

188. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

189. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians

[113] *Id.*

> who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Defendant Violated Standards Set Forth in Illinois Law.

190. Under the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), Plaintiff and Class Members have rights to privacy and confidentiality in their health care.

191. The MPRA provides:

> Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed: (1) to the patient, (2) to the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, (3) for treatment in accordance with 45 CFR 164.501 and 164.506, (4) for payment in accordance with 45 CFR 164.501 and 164.506, (5) to those parties responsible for peer review, utilization review, and quality assurance, (6) for health care operations in accordance with 45 CFR 164.501 and 164.506, (7) to those parties required to be notified under the Abused and Neglected Child Reporting Act or the Illinois Sexually Transmissible Disease Control Act, or (8) as otherwise permitted, authorized, or required by State or federal law. This right may be waived in writing by the patient or the patient's guardian or legal representative, but a physician or other health care provider may not condition the provision of services on the patient's, guardian's, or legal representative's agreement to sign such a waiver.

410 Ill. Comp. Stat. 50/3(d).

192. Furthermore, the Illinois Personal Information Protection Act ("IPIPA") protects Plaintiff's and Class Members' Medical Information and Personal Information from unauthorized disclosure. 815 Ill. Comp. Stat. 530/5, /45.

193. Defendant is a "Data Collector" and subject to the provisions of the IPIPA. *See* 815 Ill. Comp. Stat. 530/5.

194. The IPIPA provides that:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 Ill. Comp. Stat. 530/459(a).

195. Defendant's Disclosure of Plaintiff's and Class Members' Private Information to third parties, including Facebook, through the operation of the Pixel on its Website and Online Platforms, and to Google, Microsoft, AdRoll, AppNexus, HubSpot, Frequence, the Trade Desk, via their respective trackers, violated Plaintiff's and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standard for safeguarding the confidential Private Information of Plaintiff and the Class Members.

H. Plaintiff's and Class Members' Expectation of Privacy

196. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

I. IP Addresses are Personally Identifiable Information

197. On information and belief, Defendant also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

198. An IP address is a number that identifies the address of a device connected to the Internet.

199. IP addresses are used to identify and route communications on the Internet.

200. IP addresses of individual Internet users, including Defendant's patients, are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

201. Facebook tracks every IP address ever associated with a Facebook user.

202. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

203. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

204. Consequently, by disclosing the IP addresses of Plaintiff and the Class Members—patients of Defendant--Defendant's business practices violated HIPAA and industry privacy standards.

J. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

205. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

206. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

207. Retargeting is a form of online marketing that targets users, including Defendant's patients, with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

208. By utilizing the Meta Pixel and other trackers, the cost of advertising and

retargeting was reduced, thereby benefiting Defendant.

K. Plaintiff's and Class Members' Private Information Had Financial Value

209. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[114] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[115] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[116]

210. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[117]

---

[114] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).

[115] *Id.*

[116] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).

[117] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).

211. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

212. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[118]

213. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[119]

TOLLING, CONCEALMENT, AND ESTOPPEL

214. The applicable statutes of limitation have been tolled as a result of Village's knowing and active concealment and denial of the facts alleged herein.

215. Village seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing patients using those platforms with no indication that their Website usage was being tracked and transmitted to third parties. Village knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members

[118] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.

[119] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook and likely other third parties.

216. Plaintiff and Class Members could not with due diligence have discovered the full scope of Village's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology to unauthorizedly disclose their PHI/Private Information.

217. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Village's illegal interception and disclosure of Plaintiff's and the Class's Private Information has continued unabated. What is more, Village was under a duty to disclose the nature and significance of its data collection practices but did not do so. Village is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

218. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all other similarly situated persons pursuant to Fed. R. Civ. P. 23.

219. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All patients of Defendant whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

220. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

221. Plaintiff reserves the right to modify or amend the definition of the proposed class

before the Court determines whether certification is appropriate.

222. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23(a)(1)-(4).

223. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant, and the Class is identifiable within Defendant's records.

224. Ascertainability. Class Members are readily identifiable from information in Defendant's possession, custody, and control.

225. Commonality and Predominance: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately Plaintiff's and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant's conduct breached its duties of care and amounts to negligence;

j. whether Defendant was negligent *per se*;

k. whether Defendant committed invasion of privacy—intrusion upon seclusion;

l. whether Defendant breached its implied contract with Plaintiff and the Class Members; or in the alternate, whether Defendant was unjustly enriched;

m. whether Defendant breached its implied duty of confidentiality;

n. whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.;

o. whether Defendant's conduct violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.;

p. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

q. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

r. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.;

s. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

t. whether Plaintiff and the Class Members are entitled to damages, including actual, compensatory, and nominal damages;

u. the measure of Plaintiff's and the Class Members' damages; and,

v. whether Plaintiff and the Class Members are entitled to punitive damages.

226. Defendant has engaged in a common course of conduct toward Plaintiff and the Class Members, in that the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully disclosed and accessed in the same way. As set forth above, the common issues arising from Defendant's conduct affecting Class Members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

227. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

228. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct

with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

229. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

230. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

231. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably

consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

232. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

233. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

234. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure and failure to properly secure the Private Information of Plaintiff and the Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

235. Moreover, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

236. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether Defendant was negligent and/or negligent *per se*;

e. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

f. whether Defendant breached the contract;

g. in the alternate, whether Defendant was unjustly enriched;

h. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

i. whether Defendant failed to implement and maintain reasonable security procedures and practices;

j. whether Defendant invaded Plaintiff and the Class Members' privacy;

k. whether Defendant breached its implied duty of confidentiality;

l. whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.;

m. whether Defendant violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.;

n. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

o. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

p. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.;

q. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; and,

r. whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

237. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

238. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

239. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

240. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

241. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

242. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

243. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

244. Defendant's breach of its common-law duties to exercise reasonable care and negligence, directly and proximately caused Plaintiff's and Class Members' actual, tangible,

injury-in-fact and damages, including, without limitation: the unauthorized access of their Private Information by third parties; improper disclosure of their Private Information; receipt of targeted advertisements reflecting private medical information; lost benefit of their bargain; lost value of their Private Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time and money incurred to mitigate and remediate the effects of use of their information, as to targeted advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiff and the Class Members of surrendering their choices to keep their Private Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiff's and the Class Members' Private Information; and other injuries and damages as set forth herein. These injuries are ongoing, imminent, immediate, and continuing.

245. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

246. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

247. Plaintiff re-alleges and incorporates the above allegations as if fully set forth

herein.

248. Plaintiff beings this negligence *per se* count in the alternative to his common law negligence claim.

249. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, and Illinois law, including the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), and the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/5, /45, *et seq*., Defendant was required by law and industry standards to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

250. Plaintiff and Class Members are within the class of persons that these statutes and rules were designed to protect.

251. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

252. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

253. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, and others gaining

access to Plaintiff's and Class Members' PII and PHI, and resulting in Defendant's liability under principles of negligence *per se*.

254. Defendant violated its duty under Section 5 of the FTC Act and/or HIPAA by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

255. Plaintiff's and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

256. As a proximate result of Defendant's negligence *per se* and breach of duties as set forth above, Plaintiff and Class Members were caused to, *inter alia*, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their PII and PHI, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their PII and PHI, all of which can constitute actionable actual damages.

257. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

258. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff

and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT III
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

259. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

260. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms.

261. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

262. As set forth above, Defendant disclosed Plaintiff's and the Class Members' Private Information and confidential communications to Facebook and other third parties, without their authorization or knowledge.

263. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and concerns.

264. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations in its Privacy Policies and elsewhere. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

265. Defendant's Disclosure of PHI coupled with PII—Private Information—is highly

offensive to the reasonable person.

266. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights, and other injuries and damages as set forth in the preceding paragraphs.

267. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

268. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

269. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

270. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

271. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

272. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received.

273. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere,

to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. Implicit in the agreement between Defendant and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

274. Village had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

275. Defendant had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

276. Additionally, Defendant implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

277. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant. Village did not. Plaintiff and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Defendant.

278. Defendant breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties, including Facebook, Google, and others.

279. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

280. As a direct and proximate result of Defendant's breach of contract, Plaintiff and

the Class have suffered (and will continue to suffer) injury-in-fact and damages, including monetary damages; loss of privacy; unauthorized disclosure of Private Information; unauthorized access to Private Information by third parties; use of the Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of their information.

281. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

282. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

283. This claim is pleaded in the alternative to Plaintiff's breach of implied contract claim.

284. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information—Private Information—that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with third parties.

285. Plaintiff and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

286. Defendant appreciated or had knowledge of the benefits conferred upon it by

Plaintiff and Class Members.

287. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy practices and procedures that Plaintiff and Class Members paid for, and those purchases with unreasonable data privacy practices and procedures that they received.

288. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

289. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of the conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF IMPLIED DUTY OF CONFIDENTIALITY
(On Behalf of Plaintiff and the Class)

290. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

291. Plaintiff and Class Members were patients of Defendant and received healthcare services from Defendant.

292. Defendant agreed to keep Plaintiff's and Class Members' Private Information and communications confidential as part of establishing and maintaining the healthcare services in the provider/patient relationship between Defendant and Plaintiff and Class Members.

293. There is a duty of confidentiality implied in every healthcare provider and patient relationship, akin to an implied contract, such that healthcare services providers may not disclose

confidential information acquired through the healthcare provider-patient relationship.

294. The implied duty of confidentiality is at least as extensive as Defendant's statutory obligations as a healthcare services provider to maintain patient confidentiality.

295. Under the Illinois Medical Patient Rights Act, "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients." 410 Ill. Comp. Stat. 50/3.

296. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

297. Defendant may also not disclose PHI and PII about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501, 164.508(a)(3), 164.514(b)(2)(i).

298. Plaintiff and Class Members performed all required conditions of their implied contracts with Defendant.

299. Defendant breached the implied duty of confidentiality to Plaintiff and Class Members by intentionally deploying Pixels on its Website and Online Platforms that caused the transmission of Private Information including PII, PHI, and confidential communications to third parties, including Facebook.

300. Plaintiff seeks all monetary and non-monetary relief allowed by law.

COUNT VII
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.
(On Behalf of Plaintiff and the Class)

301. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

302. The Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA") makes it unlawful to employ "[u]nfair methods of competitions and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in [this section] . . . in the conduct of any trade or commerce." 815 Ill. Comp. Stat. § 505/2.

303. Defendant is a "person" as defined by 815 Ill. Comp. Stat. § 505/1.

304. Plaintiff and the Class Members are "consumers" as defined by 815 Ill. Comp. Stat. § 505/1.

305. Defendant was engaged "in the conduct of trade or commerce" by hosting and publishing its Website that it encouraged its patients to use and where it advertised their healthcare services to the public.

306. Plaintiff's and the Class Members' payments to Defendant for health care services were for household and personal purposes.

307. Defendant used unfair and deceptive acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2, including but not limited to the following.

a. Defendant encouraged its patients to use its Website and Online Platforms while representing its commitment to protecting the privacy of their Personal Information. Meanwhile, Defendant shared Plaintiff's and Class Members' Private Information with Facebook, Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, the Trade Desk, and possibly others, without Plaintiff's and Class Members' knowledge or consent.

b. Defendant promised that it would not use Plaintiff's and Class Members' PHI for undisclosed purposes without Plaintiff's and Class Members' permission. At the same time, Defendant knowingly collected Plaintiff's and Class Members' Private Information and transmitted to third parties like Facebook, exclusively for the purpose of marketing and profits. On information and belief, Defendant then used this information to market its services to Plaintiff and Class Members.

c. Plaintiff and Class Members relied on Defendant's representations in using Defendant's Online Platform and thought they were communicating only with their trusted healthcare provider. In actuality, Defendant was surreptitiously intercepting and transmitting Plaintiff's and Class Member's communications from Plaintiff's and Illinois Subclass Members' browsers directly to Facebook.

308. Defendant's Disclosure of Plaintiff and Class Members' Private Information was willful, knowing, and done with intent that Plaintiff and Class Members rely upon the concealment, suppression or omission of a material fact: that Defendant was tracking Plaintiff's and Class Members' Private Information, using it for advertising purposes without their permission, and disclosing that information to unauthorized third parties.

309. Had Plaintiff and Class Members been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to Defendant.

310. The CFDPA provides that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person.

The court, in its discretion may award actual economic damages or any other relief which the court deems proper." 815 Ill. Comp. Stat. Ann. 505/10a(a). Further, "the Court may grant injunctive relief where appropriate and may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs to the prevailing party." *Id*. at 505/10a(b).

311. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the CFDPA, Plaintiff and Class Members have suffered damages for which Defendant is liable, including, but not limited to, the following.

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private.

b. Defendant eroded the essential confidential nature of the doctor-patient relationship.

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value.

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality.

e. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

312. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the CFDPA. Had Plaintiff and Class Members been aware that their Private Information would be transmitted to unauthorized

third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to Defendant.

313. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, reasonable attorneys' fees and costs, and injunctive relief.

COUNT VIII
VIOLATION OF THE ILLINOIS EAVESDROPPING STATUTE,
720 Ill. Comp. Stat. 5/14, *et seq*.
(On Behalf of Plaintiff and the Class)

314. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

315. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 Ill. Comp. Stat. 5/14-2(a), -4.

316. The IES also states that it is a felony for any person to knowingly and intentionally "use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties." *Id*.

317. For purposes of the IES, "eavesdropping device" means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means." 720 Ill. Comp. Stat. 5/14-1(a).

318. For purposes of the IES, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 Ill. Comp. Stat. 5/14-1(g).

319. For purposes of the IES, "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device." 720 Ill. Comp. Stat. 5/14-1(e).

320. "A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution." *Id*.

321. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' private electronic communications, without the consent of Plaintiff and Class Members, using the Pixel and similar tracking technologies on its Online Platforms.

322. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' private electronic communications for the purpose of disclosing those communications to third parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

323. Plaintiff's and Class Members' communications with Defendant constitute private conversations, communications, and information.

324. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

325. Plaintiff and Class Members communicated sensitive PHI and PII that they

intended for only Defendant to receive and that they understood Defendant would keep private.

326. Plaintiff and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiff's or Class Members' authorization, consent, or knowledge.

327. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, Privacy Policies, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

328. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties, including Facebook, as they communicated with Defendant through its Online Platforms.

329. Without Plaintiff's or Class Members' knowledge, authorization, or consent, Defendant used the Pixel imbedded and concealed into the source code of its Online Platforms to secretly record and transmit Plaintiff's and Class Members' private communications to hidden third parties, such as Facebook, Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, and the Trade Desk as described in the preceding paragraphs.

330. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practices contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ." 720 Ill. Comp. Stat. 5/14-6.

331. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members' browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Other tracking technology including Google Analytics, Google Tag Manager, Google DoubleClick Ads, Microsoft Universal Events, HubSpot, AdRoll, AppNexus, Frequence, and The Trade Desk;

g. Defendant's computing servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third-parties (including Facebook) to which Plaintiff's and Class Members' communications were disclosed.

332. The eavesdropping devices outlined above are not excluded "tracking devices" as that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.

333. Defendant is a "person" under the IES. 720 Ill. Comp. Stat. 5/2-15.

334. Defendant aided in the interception of communications between Plaintiff and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiff's or Class Members' consent.

335. Under the IES, Plaintiff and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

336. Defendant's violation of the IES caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members

b. intended to remain private is no longer private;

c. Defendant eroded the essential confidential nature of the physician-patient relationship;

d. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

e. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

f. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information.

337. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IX
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. §§ 2511(1), *et seq.*
(On Behalf of Plaintiff and the Class)

338. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

339. The ECPA protects both sending and receipt of communications. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

340. The transmissions of Plaintiff's and Class Members' Private Information to

Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

341. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

342. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include [] any information concerning the substance, purport, or meaning of that communication." *See* 18 U.S.C. § 2510(8).

343. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents…include any information concerning the substance, purport, or meaning of that communication." See 18 U.S.C. § 2510(4), (8).

344. **Electronic, Mechanical or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. Defendant's Website.

345. The tracking technology deployed by Defendant effectuated the sending and acquisition of patient communications.

346. By utilizing and embedding the tracking technology on its Website, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

347. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the tracking technology including the Pixel, which tracked, stored ,and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook, Google, Microsoft, AdRoll, AppNexus, Hubspot, Frequence, and the Trade Desk, and possibly others.

348. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding Private Information, and medical treatment.

349. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

350. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

351. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely,

invasion of privacy, among others.

352. Defendant intentionally used the wire or electronic communications to increase its profit margins and save on marketing costs.

353. Defendant specifically used the Pixel to track and to utilize Plaintiff's and Class Members' Private Information for financial gain.

354. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

355. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy via the tracking technology.

356. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be highly offensive to a reasonable person; and (ii) violation of HIPAA, the FTC Act, invading Plaintiff's and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.

COUNT X
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(3)(a)
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
(On Behalf of Plaintiff and the Class)

357. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

358. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any

communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

359. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant's Website is an electronic communication service which provides to users thereof, patients of Defendant, the ability to send or receive electronic communications; in the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' Private Information.

360. **Intentional Divulgence**. Defendant intentionally designed the tracking technology and was or should have been aware that, if so configured, it could divulge Plaintiff's and Class Members' Private Information. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

361. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization and/or consent.

362. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[120] or an agent of an ECS, the ECPA states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication."

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;

[120] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;" c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." U.S.C. § 2511(3)(b).

363. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

364. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of Defendant's service nor (ii) necessary to the protection of the rights or property of Defendant.

365. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

366. Defendant's divulgence of the contents of Plaintiff's and the Class Members' patient user communications on its Website through the tracking technology was not done "with the lawful consent of the originator or any addresses or intended recipient of such

communication[s].” As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the “lawful consent” from the websites or apps with which Plaintiff and Class Members were exchanging information.

367. Moreover, Defendant divulged the contents of Plaintiff’s and Class Members’ communications through the Pixel code to individuals who are not “person[s] employed or whose facilities are used to forward such communication to its destination.”

368. The contents of Plaintiff’s and Class Members’ communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

369. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney’s fee and other litigation costs reasonably incurred.

COUNT XI
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (“STORED COMMUNICATIONS ACT”)
18 U.S.C. § 2702, *et seq.*
(On Behalf of Plaintiff and the Class)

370. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

371. The ECPA further provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

372. **Electronic Communication Service**. ECPA defines “electronic communications

service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant intentionally procures and embeds various Plaintiff's and Class Members' patient Private Information through the tracking technology used on Defendant's Website, which qualifies as an Electronic Communication Service.

373. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

374. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Website and files associated with it.

375. When Plaintiff or Class Members make a Website communication, the content of that communication is immediately placed into storage.

376. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the tracking technology.

377. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—" a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;" c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;" d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;" e. "as may be necessarily incident to the rendition of the service or to the protection

of the rights or property of the provider of that service;" f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A." g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;" h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

378. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

379. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

380. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

381. Defendant's divulgence of the contents of Plaintiff's and Class Members'

communications on its Website to Facebook or other third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii) necessary to the protection of the rights or property of Defendant.

382. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

383. Defendant's divulgence of the contents of Plaintiff's and Class Members' patient user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

384. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

385. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

386. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff and the Class)

387. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

388. Plaintiff's and the Class Members' computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

389. Defendant exceeded, and continues to exceed, authorized access to Plaintiff's and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

390. Defendant's conduct caused "loss to 1 or more persons during any 1-year period… aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' Private Information as set forth in detail herein, which were never intended for public consumption.

391. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff and the Class Members' Private Information and communication being made available to Defendant, Facebook, Google, and/or other third parties without adequate legal privacy protections.

392. Accordingly, Plaintiff and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, ANGEL RODRIGUEZ, individually, on behalf of himself, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

C. for an award of punitive damages, as allowable by law;

D. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

E. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

F. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

G. ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

H. for an award of reasonable attorneys' fees and costs under the CFDPA, the common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiff in

connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of himself, and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: July 31, 2024

Respectfully submitted,

/s/ Samuel J. Strauss

Samuel J. Strauss, Bar No. 6340331
Raina C. Borrelli
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Lynn A. Toops
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice*)
Andrew E. Mize (*Pro Hac Vice*)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com
eschiller@stranchlaw.com

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on July 31, 2024, a true and correct copy of the foregoing was served electronically by the Court's e-filing system on all counsel of record in accordance with the Rules of Civil Procedure.

/s/ Samuel J. Strauss _____

Counsel for Plaintiff and the Proposed Class